

UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF NEW YORK  
Civil Action No.: 24-4198

Hao Zhe Wang *pro se* )  
)  
)  
vs. )  
)  
AT&T Inc. and North Lane )  
Technologies Inc. )  
)  
)

**Motion to Reopen Action and to Amend**

Pursuant to the Court's July 24 Order of Dismissal (Dkt 20), which gave parties additional time to attempt to complete their settlement talk but also gave Plaintiff the right to reopen the case if the settlement discussion fails, Plaintiff respectfully asks to reopen the instant action.

While the Court generously gave parties extra time to complete their settlement negotiations, there is a statutory deadline for a party to file a motion under 9 U.S. Code § 12, and on its face the Court's July 24 Order does not extend the statutory deadline for a Section 12 motion. Nor does the Second Circuit recognize a trial court's authority to extend the statutory deadline stipulated in the *Federal Arbitration Act*. As such, Plaintiff does not believe it is meaningful or rewarding to seek more time from the Court to further stretch out the settlement talk.

Therefore, Plaintiff asks for the action to be reopened.

Separately, Defendant AT&T also informed Plaintiff last month that the metadata of his mobile account, including call and text records, “were accessed by cybercriminals.” Over the past few weeks, parties have not been able to agree on how to reserve parties’ litigation rights in relation to the hack of Plaintiff’s call and text logs in the tentative settlement parties had reached earlier. Plaintiff respectfully asks for the Court’s leave for him to amend his complaint to add allegations and claims related to the recently disclosed hack.

Significantly, the information in Plaintiff’s AT&T account that was hacked this time is *not* duplicative of Plaintiff’s account information that AT&T shared with Defendant North Lane in 2022. The latest hack concerned his call and text logs (see <https://www.att.com/support/article/my-account/000102979>), whereas the account information AT&T shared with its Russian-spy-infested vendor concerned Plaintiff’s contact, biographic, and financial information (Complaint, ¶¶33, 35).

Whereas businesses have frequently been caught being negligent and reckless in collecting, storing, and handling highly sensitive customer, it is usually the biographic and financial information that was accessed and peddled on the dark web by criminals. In turn, businesses have offered a common remedy for their customers whose biographic and financial information was stolen from their digital vaults: paying for the victims’ identity theft insurance and paying for their credit monitoring.

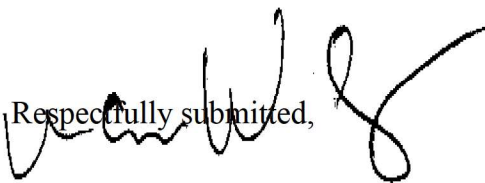
Thus far, AT&T has offered no similar remedy to Plaintiff or other AT&T customers for the hack of their call and text logs. For no easy remedy exists in the event of a phone metadata leak. Cybercriminals who get hold of the call log of a victim immediately learn which numbers she contacts most often and are her trusted numbers. The criminals can easily spoof one of those trusted numbers and impersonate her bank or brokerage or family members and can trick her into

wiring all the money in her 401k to Russia. Simply put, when criminals know which phone numbers the victim trusts, no amount of education, experience and intelligence can shield the victim from being deceived and defrauded. This is why businesses have not successfully fashioned a remedy for leaked call logs.

Plaintiff also considers the theft of his call and text logs especially harmful. Among those AT&T customers whose call and text metadata were stolen, Plaintiff also stands out for his particular vulnerability because AT&T had previously shared the other half of the puzzle for the cybercriminals – Plaintiff's biographic and financial information – with an organization that is reported to have been infiltrated and managed by Russian intelligence operatives. Moreover, on top of the risk of theft and financial fraud, which will likely last for the rest of his life, the metadata could reveal Plaintiff's various social and political affiliations that once made him and his family a target of stalking and racist assaults.

As such, Plaintiff asks for the Court's leave to amend his complaint to include allegations and claims related to the leak of the metadata of his phone communications that AT&T notified him of last month. Plaintiff expects to need two weeks of time to do so.

Respectfully submitted,

A handwritten signature in black ink, appearing to be 'V. W. S.', is written over the text 'Respectfully submitted,'.